

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ERIN K. MAUDE,
Plaintiff,
v.
DOES 1 THROUGH 10,
Defendant.

Case No. [21-cv-08353-VKD](#)

**ORDER DENYING WITHOUT
PREJUDICE EX PARTE MOTION FOR
EXPEDITED DISCOVERY**

Re: Dkt. No. 6

Plaintiff Erin Maude moves ex parte for an order authorizing service of subpoenas on three internet service providers (“ISPs”) so that she may obtain documents identifying the unnamed defendants in this action. Dkt. No. 6. The Court deems this motion suitable for determination without oral argument. Civil L.R. 7-1(b).

Because Ms. Maude has not demonstrated good cause for the proposed discovery, the Court denies the motion without prejudice.

I. BACKGROUND

Ms. Maude filed this action on October 27, 2021 alleging that unknown persons accessed her computers, electronic devices, and online accounts in violation of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, and California Penal Code § 502. Dkt. No. 1. She claims that in or around August 2020, she discovered that information and messages had been deleted from her mobile telephone, and that unauthorized devices had accessed her computer system and certain of her online accounts. *Id.* ¶¶ 10-30. Ms. Maude pleads all claims against “John and Jane Does 1 through 10, John Doe Corporations 1 through 10, and Other John Doe Entities 1 through 10” (collectively, “Doe defendants”). *Id.* ¶¶ 3-7. She says that she is unaware

of the true identities of the Doe defendants, and so no summons or complaint has been served.
Dkt. No. 6 at 2.

Ms. Maude has identified several IP addresses she believes have been used to access her computer system without permission, as well as several MAC addresses corresponding to devices that have obtained unauthorized access to her computer system. She explains that she has attempted to obtain information informally from various service providers in an effort to stop the unauthorized access to her computer system, devices, and accounts. *See generally* Dkt. No. 9. She also relies on the declaration of Joseph Manship, a technical consultant, who attests in relevant part that after reviewing information provided by Ms. Maude, including “the physical location of Internet Protocol addresses logged as accessing her email account,” he believes that there has been unauthorized access to Ms. Maude’s email and social media accounts. *See* Dkt. No. 8 ¶ 4.

Ms. Maude wishes to subpoena the ISPs that control the IP addresses associated with incidents of unauthorized access to her computer system for information that may be used to identify the ISP customers who use the IP addresses at issue. *Id.* Specifically, Ms. Maude seeks to subpoena the following documents:

Any document identifying the [ISP] customer using the Internet Protocol address [XXXX] on [date and time], including the name, address, telephone number, email address and Media Access Control (“MAC”) address associated with use of the Internet Protocol address.¹

See Dkt. No. 7, Ex. A.

II. DISCUSSION

Generally, a party may not obtain discovery “from any source” before initiation of the Rule 26(f) conference, let alone before service of the summons and complaint. Fed. R. Civ. P. 26(d)(1); *Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 577 (N.D. Cal. 1999). However, where a plaintiff demonstrates good cause, a court may order early discovery. *See, e.g., Distinct Media*

¹ Ms. Maude’s counsel explains that he intends to issue subpoenas “specific to [each ISP’s] Internet Protocol address” and “would use the most recent date and time of intrusion so that the ISP is likely to have not yet destroyed the relevant evidence.” Dkt. No. 7 ¶ 4.

Ltd. v. Doe Defendants 1-50, No. 15-cv-03312 NC, 2015 WL 13389609, at *2 (N.D. Cal. Sept. 29, 2015). In particular, where a plaintiff requires discovery in order to identify unknown defendants, early discovery may be appropriate. *See id.*; *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980) (“[S]ituations arise . . . where the identity of alleged defendants will not be known prior to the filing of a complaint. In such circumstances, the plaintiff should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds.”).

In evaluating whether a plaintiff establishes good cause for expedited discovery of defendants’ identities, courts in the Ninth Circuit consider whether the plaintiff: (1) has identified the missing defendant with sufficient specificity such that the court can determine that the defendant is a real person or entity who could be sued in federal court, (2) has described the previous steps taken to locate the missing defendant, (3) established that the action can withstand a motion to dismiss, and (4) demonstrated a reasonable likelihood that discovery will yield identifying information about the defendant that would make service of process possible. *See Bungie, Inc. v. Thorpe*, No. 21-cv-05677-EMC (DMR), 2021 WL 5178825, at *3 (N.D. Cal. Nov. 8, 2021) (collecting cases); *Columbia Ins. Co.*, 185 F.R.D. at 578-80 (discussing relevant considerations).

Ms. Maude’s motion for expedited discovery does not cite or specifically address the relevant considerations for evaluating a request for pre-service discovery. Nevertheless, the Court considers the matters presented in her motion in view of the applicable framework for decision.

A. Identification of Missing Defendants with Sufficient Specificity

The Court first considers whether Ms. Maude has identified the missing defendants with sufficient specificity. “This requirement is necessary to ensure that federal requirements of jurisdiction and justiciability can be satisfied.” *Columbia Ins. Co.*, 185 F.R.D. at 578. In addition, courts examining this factor have considered whether the plaintiff has shown that the court likely will have personal jurisdiction over the missing defendants. *See Bungie*, 2021 WL 5178825, at *3 (collecting cases).

Here, Ms. Maude has shown that the missing defendants are likely actual people. She

describes unauthorized access to her computer system and online accounts by specific, unauthorized personal electronic devices, suggesting that an actual user (or users) of such devices has deliberately engaged in the alleged misconduct. Ms. Maude has also shown that at least some of the missing defendants are likely to be subject to the personal jurisdiction of the Court, given the nature of the misconduct alleged and Ms. Maude's declaration that "[t]here were three IP addresses which were assigned to a private Comcast user in Monterey [in] late January and early February 2021 and these three IP addresses [accessed her Hotmail email account] late at night in a city [she] was not in at those times." Dkt. No. 9 ¶ 8. However, as explained in more detail below, it is not clear whether the IP addresses for which Ms. Maude seeks discovery correspond to a user or users located within the jurisdiction of this Court because she has not provided that information to the Court.

B. Previous Steps Taken to Locate Missing Defendants

The Court next considers whether Ms. Maude has described the steps already taken to locate the missing defendants. "This element is aimed at ensuring that plaintiff[] make[s] a good faith effort to comply with the requirements of service of process and specifically identifying defendants." *Columbia Ins. Co.*, 185 F.R.D. at 579.

Ms. Maude's motion describes at length the basis for her contention that someone has obtained unauthorized access to her computer system, electronic devices, and online accounts. However, the motion says very little regarding her previous efforts to identify and locate the missing defendants. She and Mr. Manship refer in passing to the use of IP address location tools (*see* Dkt. No. 8 ¶ 4; Dkt. No. 9 ¶ 8), but their declarations do not describe the efforts undertaken, using these location tools or otherwise, to identify the users of the IP addresses at issue or their geographic locations. *Cf. Distinct Media*, 2015 WL 13389609, at *3 ("A court may find insufficient effort, however, when a plaintiff consults only with the publicly available WhoIs domain name directory and does not contact anyone listed in the directory."). For this reason, the Court concludes that Ms. Maude does not satisfy this requirement.

C. Whether the Action Could Withstand a Motion to Dismiss

The third factor requires the Court to consider whether the complaint would survive a

1 motion to dismiss. “[P]laintiff must make some showing that an act giving rise to civil liability
2 actually occurred and that the discovery is aimed at revealing specific identifying features of the
3 person or entity who committed that act.” *Columbia Ins. Co.*, 185 F.R.D. at 580.

4 Ms. Maude’s first claim for relief asserts a violation of the CFAA against all defendants.
5 While the CFAA is principally a criminal statute, a private civil right of action is available. *See* 18
6 U.S.C. § 1030(g); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009) (“[A]
7 private plaintiff must prove that the defendant violated one of the provisions of § 1030(a)(1)-(7),
8 and that the violation involved one of the factors listed in [the relevant statutory subsection].”).
9 Ms. Maude does not identify which provision or provisions of the CFAA defendants violated. In
10 her motion, she merely asserts, without elaboration, that she “has pled the elements of the causes
11 of action and has provided evidence . . . for each element.” Dkt. No. 6 at 8. This is insufficient,
12 and in these circumstances, the Court concludes that her CFAA claim is unlikely to survive a
13 motion to dismiss. *See Distinct Media*, 2015 WL 13389609, at *4 (“Given the complexity of the
14 statute and the Ninth Circuit’s requirement to address specific statutory provisions, the Court finds
15 that [plaintiff’s] complaint fails to provide defendants with ‘fair notice of what the . . . claim is and
16 the grounds upon which it rests.’”) (citation omitted).

17 Ms. Maude’s second claim for relief asserts a violation of California Penal Code § 502
18 against all defendants. Like the CFAA, § 502 is a criminal statute, but also provides for a private
19 civil right of action for damage or loss based on a violation of one or more of the specific
20 provisions of subdivision (c) of the statute, which enumerates fourteen different acts of
21 misconduct. *See* Cal. Penal Code § 502(e)(1). Ms. Maude’s complaint does not identify which
22 provisions of § 502 form the basis for her second claim for relief. For reasons similar to those
23 applicable to her CFAA claim, the Court concludes that Ms. Maude’s second claim for relief also
24 does not give fair notice of the grounds on which it rests and is therefore unlikely to survive a
25 motion to dismiss. *See Distinct Media*, 2015 WL 13389609, at *4.

26 **D. Whether Discovery Will Yield Identifying Information**

27 The fourth factor requires the Court to consider whether the discovery requested is
28 reasonably likely to lead to identifying information about the missing defendants that would make

1 service of process possible. *Columbia Ins. Co.*, 185 F.R.D. at 580.

2 Ms. Maude argues that the discovery she requests is “narrowly tailored.” Dkt. No. 6 at 7.
3 Specifically, she says that she “asks only that the ISPs that control the IP addresses associated with
4 the unauthorized access to [her] computer systems be lawfully allowed to reveal the identities of
5 the customers using the IP addresses at specific times.” *Id.* Ms. Maude’s motion does not identify
6 the three ISPs from whom she wishes to obtain discovery. Her proposed order refers to the ISPs
7 “listed in the complaint.” Dkt. No. 10 at 2. The complaint identifies “Comcast Corporation, Aqua
8 Networks Limited, and AT&T Services, Inc.” as the ISPs who control the IP addresses at issue.
9 Dkt. No. 1 ¶¶ 18-20. However, the “model” subpoena attached to the declaration of her counsel,
10 Mr. Walton, is directed to only one ISP, “Comcast Cable Communications, LLC,” which is not
11 identified in the complaint. *See* Dkt. No. 7, Ex. A.

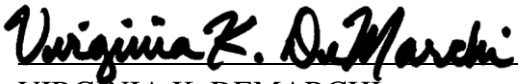
12 The Court cannot properly evaluate Ms. Maude’s proposed subpoenas unless she files
13 them with the Court. In addition, Ms. Maude fails to demonstrate that the IP addresses for which
14 she seeks identifying information relate to her claims against the missing defendants and that the
15 discovery is tailored to obtaining only the information necessary to identify the missing defendants
16 for purposes of service of process. *See, e.g., Ebates, Inc. v. Does 1-211*, No. 16-cv-01925-JST,
17 2016 WL 2344199, at *3 (N.D. Cal. May 3, 2016) (discussing fourth factor and limiting scope of
18 proposed subpoena). For this reason, Ms. Maude does not satisfy the fourth requirement.

19 **III. CONCLUSION**

20 For the reasons explained above, the Court denies the motion for expedited discovery
21 without prejudice. Ms. Maude may amend her complaint and renew her motion to address the
22 matters discussed above.

23 **IT IS SO ORDERED.**

24 Dated: November 22, 2021

25
26 
27 VIRGINIA K. DEMARCHI
28 United States Magistrate Judge